

Secure quantum conversation through non-destructive discrimination of highly entangled multipartite states

Sakshi Jain

*Indian Institute of Technology-Bombay, Mumbai - 400076, India**

Sreraman Muralidharan

*Department of Information and communication technology,
Royal Institute of Technology(KTH), SE-164 40 Kista, Sweden†*

Prasanta K. Panigrahi‡

*Indian Institute of Science Education and Research Kolkata, Mohanpur Campus,
BCKV Campus Main Office, Mohanpur - 741252, India and
Physical Research Laboratory, Navrangpura, Ahmedabad - 380 009, India*

“Quantum conversation” is a way in which two parties can communicate classical information with each other using entanglement as a shared resource. We present this scheme using a multipartite entangled state after describing its generation through appropriate circuit diagrams. We make use of a discrimination scheme which allows one to perform a measurement on the system without destroying its entanglement. We later prove that this scheme is secure in a noiseless and a lossless quantum channel.

PACS numbers: 03.67.Hk, 03.65.Ud

Keywords: Entanglement, Non-destructive discrimination, Quantum dialogue

I. INTRODUCTION

Quantum cryptography [1, 2, 3] is one of the significant applications of quantum information theory, which has also been experimentally realized in various systems [4, 5]. It enables one to transmit secret messages between various parties with unconditional security. Quantum secure direct communication (QSDC) [6] is an important branch of quantum cryptography, which uses entanglement as a resource to transmit quantum information in a secure manner, without establishing a random key. In recent years, several QSDC schemes, involving EPR pairs [7] and multiparticle entangled channels [8, 9] have been investigated. Most of these protocols involve joint measurements to be carried out on an entangled basis which is a non-trivial task. Instead, measurements on a product basis is often preferred [10]. However, this disturbs the entanglement of the system and makes the state unusable for further applications. Instead, approaches based on non-destructive discrimination (NDD) can be more useful as it enables discrimination between orthogonal quantum states by allowing a product basis measurement without destroying the entanglement of the system [11, 12, 13, 14].

Characterization of entanglement of greater than four qubits under LOCC is still an unsolved problem. However, approaches based on numerical optimization procedures to find higher qubit entangled states have recently attracted attention [15, 16, 17]. First such procedure was studied by Brown *et al.* [15], who arrived at a “highly entangled” five qubit state given by,

$$|\psi_5\rangle = \frac{1}{2}(|001\rangle|\phi_-\rangle + |010\rangle|\psi_-\rangle + |100\rangle|\phi_+\rangle + |111\rangle|\psi_+\rangle), \quad (1)$$

where $|\psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\phi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are the Bell states. This result was verified by yet another numerical procedure carried out later [16]. This state is maximally “persistent” [18] and shows a high degree of “connectedness” [19], which is an indication of genuine multiparticle entanglement. Further, it assumes the same form for all ten $(3+2)$ splits. It was shown that, $|\psi_5\rangle$ can be used for perfect teleportation and state sharing of an arbitrary two qubit state [20]. This state can also be physically realized in a cavity QED system, which is insensitive

*Electronic address: sakshi.r.jain@gmail.com

†Electronic address: sreraman@kth.se

‡Electronic address: prasanta@prl.res.in

to both cavity decay and thermal field [21]. The dense coding [22] capacity of this state reaches the ‘‘Holevo bound’’, thereby allowing the transmission of five classical bits using three qubits by consuming only two ebits of entanglement [20]. In this paper, we use the dense coding protocol and an efficient NDD scheme to set up a quantum conversation between two parties. We later prove that this protocol is secure under ideal conditions.

For the sake of completeness, we shall discuss the dense coding protocol using $|\psi_5\rangle$ as a shared entangled resource [20]. Initially Alice and Bob possess, the first three and the last two qubits of $|\psi_5\rangle$ respectively. Suppose Alice has a secret message ‘‘ $m_1m_2m_3m_4m_5$ ’’ where $m_i \in \{0, 1\}$ which she wants to send to Bob. To achieve this purpose, Alice operates unitarily on her first three qubits as,

$$((\zeta^1.\zeta^2.\zeta^3.\zeta^4.\zeta^5) \otimes \mathbf{I} \otimes \mathbf{I})|\psi_5\rangle = |\psi_5\rangle_{\mathbf{m}_1\mathbf{m}_2\mathbf{m}_3\mathbf{m}_4\mathbf{m}_5}. \quad (2)$$

$$\begin{aligned} \zeta^1 &= \sigma_x \otimes I \otimes I, \text{ if } m_1 = 1, \\ &= I \otimes I \otimes I, \text{ if } m_1 = 0, \\ \zeta^2 &= I \otimes I \otimes \sigma_x, \text{ if } m_2 = 1, \\ &= I \otimes I \otimes I, \text{ if } m_2 = 0, \\ \zeta^3 &= \sigma_z \otimes \sigma_z \otimes I, \text{ if } m_3 = 1, \\ &= I \otimes I \otimes I, \text{ if } m_3 = 0, \\ \zeta^4 &= \sigma_x \otimes I \otimes \sigma_x, \text{ if } m_4 = 1, \\ &= I \otimes I \otimes I, \text{ if } m_4 = 0, \\ \zeta^5 &= I \otimes \sigma_x \otimes \sigma_x, \text{ if } m_5 = 1, \\ &= I \otimes I \otimes I, \text{ if } m_5 = 0. \end{aligned} \quad (3)$$

For example, if Alice wants to send the 5 bit classical information ‘‘10010’’ to Bob, the unitary operation that Alice would apply on her qubits would be;

$$((\sigma_x \otimes \mathbf{I} \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I})(\sigma_x \otimes \mathbf{I} \otimes \sigma_x)(\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I})) \otimes \mathbf{I} \otimes \mathbf{I} |\psi_5\rangle = (|\psi_5\rangle_{100010}) \quad (4)$$

After performing the unitary operations in the above stated manner, Alice sends the three qubits to Bob. Bob, on receiving Alice’s qubits, performs a joint five partite von-Neumann measurement in the $|\psi_5\rangle_{\mathbf{m}_1\mathbf{m}_2\mathbf{m}_3\mathbf{m}_4\mathbf{m}_5}$ basis and distinguishes these states, thereby obtaining the message encoded by Alice.

The present scheme for bidirectional ‘‘quantum conversation’’ consists of five main steps. In the first and the second step, we generate the entangled state and initialize the protocol for a security check. In the third step, an eavesdropper’s check on the multiqubit quantum channel is performed. Later, we propose a scheme to discriminate between the 32 orthogonal $|\psi_5\rangle_{\mathbf{m}_1\mathbf{m}_2\mathbf{m}_3\mathbf{m}_4\mathbf{m}_5}$ states after implementing the dense coding protocol thereby allowing the quantum conversation to be established. Subsequently, we check for the security of the presented protocol.

II. QUANTUM CONVERSATION

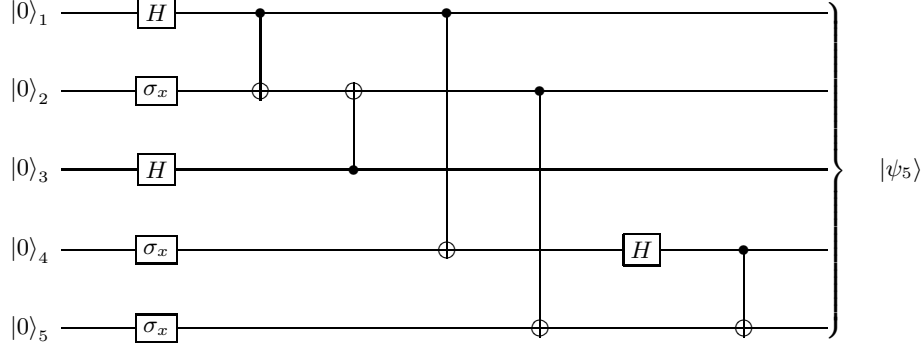
A. Generation and Initialization

Here, we describe an explicit circuit diagram for the generation of the Brown *et al.* state - a state which was obtained only through numerical searches in the past. As is evident from Fig.1, by changing the input $|00000\rangle$ to a different computational basis, 32 orthogonal Brown *et al.*, can be obtained. The above circuit makes the Brown *et al.*, state experimentally realizable in NMR and quantum dot systems.

In our quantum conversation protocol, Alice first prepares an ordered sequence of N copies of the five qubit Brown *et al.*, state $|\psi_5\rangle$: $[(q_1^1, q_2^1, q_3^1, q_4^1, q_5^1), (q_1^2, q_2^2, \dots, q_5^N)]$. Here the subscripts represent five different qubits in $|\psi_5\rangle$ and the superscripts indicate sequential ordering of the N different Brown *et al.*, states. Alice then takes the same one qubit from each $|\psi_5\rangle$ to form five ordered sequences corresponding to the five qubits, generically written as,

$$S_k = [q_k^1, q_k^2, q_k^3, \dots, q_k^N]. \quad (5)$$

Subsequently, she keeps the particle sequences S_1, S_2, S_3 and transmits the sequences S_4 and S_5 to Bob.

FIG. 1: Circuit diagram for the generation of $|\psi_5\rangle$ 

B. Measurement basis of Alice and Bob

Interestingly, the state $|\psi_5\rangle$ can be written down in two different forms as:

$$|\psi_5\rangle_{12345} = \frac{1}{2}(|001\rangle|\phi_-\rangle + |010\rangle|\psi_-\rangle + |100\rangle|\phi_+\rangle + |111\rangle|\psi_+\rangle)_{12345}, \quad (6)$$

$$|\psi_5\rangle_{13245} = ([|\phi_+\rangle|1\rangle + |\psi_+\rangle|0\rangle]|0+\rangle + [|\phi_+\rangle|1\rangle - |\psi_+\rangle|0\rangle]|0-\rangle)]_{13245} - [|\phi_-\rangle|1\rangle + |\psi_-\rangle|0\rangle]|1+\rangle + [|\phi_-\rangle|1\rangle - |\psi_-\rangle|0\rangle]|1-\rangle). \quad (7)$$

Alice and Bob exploit this characteristic of $|\psi_5\rangle$ to check the presence of an eavesdropper. It can be noted that if one measures the qubits 4 and 5 by projection on the Bell basis, i.e., say BMB_1 (Bob's Measurement Basis-1), the first three qubits of Alice would collapse into one of the computational basis $(|001\rangle, |010\rangle, |100\rangle, |111\rangle)_{123}$

which now forms the corresponding basis of Alice's measurement (AMB_1). On the other hand, if the state $|\psi_5\rangle$ is written as in equation (7), it can be observed that if Bob measures his two qubits in the basis (BMB_2): $|0+\rangle_{45}, |0-\rangle_{45}, |1+\rangle_{45}, |1-\rangle_{45}$, corresponding Alice's measurement basis (AMB_2) would be:

$(|\phi_+\rangle|1\rangle + |\psi_+\rangle|0\rangle)_{132}, (|\phi_+\rangle|1\rangle - |\psi_+\rangle|0\rangle)_{132}, (-|\phi_-\rangle|1\rangle - |\psi_-\rangle|0\rangle)_{132}$ and $(|\phi_-\rangle|1\rangle - |\psi_-\rangle|0\rangle)_{132}$. Utilizing this feature, Alice and Bob can design a defence strategy to guard against eavesdropping in the transmission. An explicit description of this strategy is given below.

C. Eavesdropping check

Bob chooses randomly a sufficiently large subset (called the sample subset) of the pair of qubits 4 and 5 from the sequences S_4 and S_5 and measures them either in the basis BMB_1 or BMB_2 . He then tells Alice the position of these pairs and the corresponding chosen measurement basis through a classical channel. Alice then measures the set of qubits 1, 2, 3 from the sequences S_1, S_2, S_3 in the corresponding basis AMB_1 or AMB_2 . Finally Alice and Bob check their measurement outcomes to find whether the quantum channel is altered. Later, they apply a majority voting technique to determine the error rate. If it turns out to be considerably high, they discard the sample subset and abort the protocol. Else, they will securely use the remaining entangled pairs of shared $|\psi_5\rangle$ to communicate their secret messages as in the next step.

D. Dense coding and NDD

The secret message " $m_1m_2m_3m_4m_5$ " is encoded by Alice in her three qubits by applying the corresponding local unitary operations as in the dense coding protocol described earlier and sent to Bob. On receiving Alice's qubits, Bob applies non-destructive discrimination (NDD) on the five qubit Brown *et al.*, state thus obtained and decodes the message without disturbing the entanglement of the system. In order to achieve this, he operates on the system through the circuit diagram shown in Fig.2, to discriminate between the 32 orthogonal Brown states non-destructively. **The outcome of the circuit with the input state as $|\psi_5\rangle_{m_1m_2m_3m_4m_5}$ can be written in general as $|\psi_5\rangle_x|x\rangle$ where $|x\rangle$ is given by, $|m_1m_2m_3m_4m_5\rangle$ and $|\psi_5\rangle_x$ is given by, $|\psi\rangle_{m_1m_2m_3m_4m_5}$.** Thus, Bob now measures the ancillas in the product basis and thereby obtains the classical message.

as,

$$|\varphi\rangle_{132E45} = (|\mu_1\rangle|\phi_+\rangle + |\mu_2\rangle|\psi_+\rangle + |\mu_3\rangle|\phi_-\rangle + |\mu_4\rangle|\psi_-\rangle)_{132E45} \quad (10)$$

where,

$$\begin{aligned} |\mu_1\rangle_{132E} &= (|\phi_+\rangle|1\rangle|\eta_{00}\rangle + |\psi_+\rangle|0\rangle|\eta_{10}\rangle - |\psi_-\rangle|0\rangle|\eta_{20}\rangle \\ &\quad - |\phi_-\rangle|1\rangle|\eta_{30}\rangle) + (|\phi_+\rangle|1\rangle|\eta_{03}\rangle + |\psi_+\rangle|0\rangle|\eta_{13}\rangle \\ &\quad - |\psi_-\rangle|0\rangle|\eta_{23}\rangle - |\phi_-\rangle|1\rangle|\eta_{33}\rangle), \\ |\mu_2\rangle_{132E} &= (|\phi_+\rangle|1\rangle|\eta_{01}\rangle + |\psi_+\rangle|0\rangle|\eta_{11}\rangle - |\psi_-\rangle|0\rangle|\eta_{21}\rangle \\ &\quad - |\phi_-\rangle|1\rangle|\eta_{31}\rangle) + (|\phi_+\rangle|1\rangle|\eta_{02}\rangle + |\psi_+\rangle|0\rangle|\eta_{12}\rangle \\ &\quad - |\psi_-\rangle|0\rangle|\eta_{22}\rangle - |\phi_-\rangle|1\rangle|\eta_{32}\rangle), \\ |\mu_3\rangle_{132E} &= (|\phi_+\rangle|1\rangle|\eta_{00}\rangle + |\psi_+\rangle|0\rangle|\eta_{10}\rangle - |\psi_-\rangle|0\rangle|\eta_{20}\rangle \\ &\quad - |\phi_-\rangle|1\rangle|\eta_{30}\rangle) - (|\phi_+\rangle|1\rangle|\eta_{03}\rangle + |\psi_+\rangle|0\rangle|\eta_{13}\rangle \\ &\quad - |\psi_-\rangle|0\rangle|\eta_{23}\rangle - |\phi_-\rangle|1\rangle|\eta_{33}\rangle), \\ |\mu_4\rangle_{132E} &= (|\phi_+\rangle|1\rangle|\eta_{01}\rangle + |\psi_+\rangle|0\rangle|\eta_{11}\rangle - |\psi_-\rangle|0\rangle|\eta_{21}\rangle \\ &\quad - |\phi_-\rangle|1\rangle|\eta_{31}\rangle) - (|\phi_+\rangle|1\rangle|\eta_{02}\rangle + |\psi_+\rangle|0\rangle|\eta_{12}\rangle \\ &\quad - |\psi_-\rangle|0\rangle|\eta_{22}\rangle - |\phi_-\rangle|1\rangle|\eta_{32}\rangle). \end{aligned} \quad (11)$$

Comparing equation (8) with (4), we arrive at the following conditions, which should be satisfied in order to avoid introducing error in the measurements:

$$\begin{aligned} \langle 001|\mu_1\rangle &= \langle 100|\mu_1\rangle = \langle 111|\mu_1\rangle = 0, \\ \langle 111|\mu_2\rangle &= \langle 001|\mu_2\rangle = \langle 010|\mu_2\rangle = 0, \\ \langle 111|\mu_3\rangle &= \langle 100|\mu_3\rangle = \langle 010|\mu_3\rangle = 0, \\ \langle 111|\mu_4\rangle &= \langle 001|\mu_4\rangle = \langle 100|\mu_4\rangle = 0. \end{aligned} \quad (12)$$

Solving the equations (9) and (10), we obtain the following conditions on the ancilla states.

$$\begin{aligned} |\eta_{00}\rangle &= |\eta_{33}\rangle, & |\eta_{03}\rangle &= |\eta_{10}\rangle, \\ |\eta_{22}\rangle &= |\eta_{11}\rangle, & |\eta_{21}\rangle &= |\eta_{12}\rangle, \\ |\eta_{20}\rangle &= |\eta_{23}\rangle = |\eta_{10}\rangle = |\eta_{13}\rangle = \mathbf{0}, \\ |\eta_{02}\rangle &= |\eta_{01}\rangle = |\eta_{32}\rangle = |\eta_{31}\rangle = \mathbf{0}. \end{aligned} \quad (13)$$

where $\mathbf{0}$ is a null ket.

Similarly, the second case is solved where Alice measures in the basis AMB_2 , and Bob measures in the basis BMB_2 and the following constraints are obtained.

$$\begin{aligned} |\eta_{00}\rangle &= |\eta_{22}\rangle, & |\eta_{13}\rangle &= |\eta_{31}\rangle, \\ |\eta_{11}\rangle &= |\eta_{33}\rangle, & |\eta_{02}\rangle &= |\eta_{20}\rangle, \\ |\eta_{01}\rangle &= |\eta_{03}\rangle = |\eta_{21}\rangle = |\eta_{23}\rangle = \mathbf{0}, \\ |\eta_{10}\rangle &= |\eta_{12}\rangle = |\eta_{30}\rangle = |\eta_{32}\rangle = \mathbf{0}. \end{aligned} \quad (14)$$

Since both the cases must be satisfied, ancilla qubits must obey both equations (11) and (12) simultaneously. As a result, the entire state reduces to, $|\varphi\rangle = |\psi_5\rangle|\eta_{00}\rangle_E$. From the above equation it is evident that the state $|\varphi\rangle$ is reduced to a product of $|\psi_5\rangle$ and the ancilla. This implies that Eve cannot gain any information about Alice's secret message by measuring the ancillas. Consequently, it can be deduced that the protocol is secure in the conditions, where there are no losses or noises in the quantum channel.

IV. CONCLUSION

In conclusion, we have presented a secure “quantum conversation” (of classical information) scheme involving dense coding through highly entangled five qubit states as the quantum channel. We describe appropriate circuits for the generation of these states which were achieved only through numerical searches in the past. This was carried out using NDD of 32 orthogonal Brown *et al.*, states. We also constructed explicit circuit diagrams for the same. Later, we proved that our schemes are secure to eavesdropper's attack in ideal conditions. In future, we wish to make a detailed analysis on the type of states that can be used for “quantum conversation” schemes.

Acknowledgments

The authors acknowledge the NIUS programme undertaken by Homi Bhabha Center for Science Education (HBCSE-TIFR) and Prof. Vijay Singh of HBCSE for encouragement and discussions. SJ and SM also acknowledge the warm hospitality of the Indian Institute of Science Education and Research (Kolkata), India, where the work was completed.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
 - [2] M. Hillery, V. Buzek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
 - [3] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [4] S. Groeblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, *New. Jour. Phys.* **74**, 145 (2002).
 - [5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **75**, 8 (2006).
 - [6] A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, *Acta. Phys. Polon. A* **101**, 357 (2002).
 - [7] K. Bostroem and T. Felbinger, *Phys. Rev. Lett.* **89**, 187902 (2002).
 - [8] H. Lee, J. Lim, and H. J. Yang, *Phys. Rev. A* **73**, 042305 (2006).
 - [9] S. Lin, Q. Y. Wen, F. Gao, and F.C. Zhu *Phys. Rev. A* **78**, 064304 (2008).
 - [10] M. A. Nielsen, E. Knill, and R. Laflamme, *Nature* **96**, 52 (1998).
 - [11] S. Muralidharan, S. Jain, S. Prasath, and P. K. Panigrahi, eprint quant-ph/0906.2147.
 - [12] R. Cleve and Gottesman, eprint quant-ph/9607030.
 - [13] M. Grassl, M. Roetteler, and T. Beth, eprint quant-ph/0211014.
 - [14] M. Gupta, A. Pathak, R. Srikanth, and P. K. Panigrahi, *Int. jour. Quantum. info.* **5**, 627 (2007).
 - [15] I. D. K. Brown, S. Stepney, A. Sudbery, and S. L. Braunstein, *J. Phys. A: Math. Gen.* **38**, 1119 (2005).
 - [16] A. Borrás, A. R. Plastino, J. Batle, C. Zander, M. Casas, and A. Plastino, *J. Phys. A: Math. Gen.* **40**, 13407 (2007).
 - [17] J. E. Tapiador, J. C. H. Castro, J. A. Clark, and S. Stepney, eprint quant-ph/0904.3874v1.
 - [18] H. J. Briegel and R. Raussendorf, *Phys. Rev. Lett.* **86**, 910 (2001).
 - [19] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
 - [20] S. Muralidharan and P. K. Panigrahi, *Phys. Rev. A* **77**, 032321 (2008).
 - [21] X. W. Wang, Z. H. Peng, C. X. Jia, Y. H. Wang, and X. J. Liu, *Opt. Commun.* **282**, 670 (2009).
 - [22] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).